



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/485,352	03/13/2000	Michael DUPRE	2643/OG629	1819

7590 07/12/2004
Christa Hildebrand
NORRIS, McLAUGHLIN & MARCUS, P.A.
220 East 42nd Street
30th Floor
NEW YORK, NY 10017

EXAMINER

TRAN, ELLEN C

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 07/12/2004

12

Please find below and/or attached an Office communication concerning this application or proceeding.

SL

Office Action Summary

Application No.

09/485,352

Applicant(s)

DUPRE, MICHAEL

Examiner

Ellen C Tran

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 14 April 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 14-26 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 14-26 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

Art Unit: 2134

DETAILED ACTION

1. This action is responsive to communication: response filed on 14 April 2004, with an original application filing date of 14 March 2000 with a foreign priority date of 4 August 1997. Claims 14, 15, 18, 19, 20, and 22 have been amended and claims 23-26 have been added.
2. Claims 1-13 withdrawn from consideration indicated in pre-amendment, 4 February 2000.
3. Claims 14-26 are currently pending in this application. Claims 14 and 19 are independent claims.

Response to Amendment

4. The amendment to the claims filed on 14 April 2004 does not comply with the requirements of 37 CFR 1.121(c) because the amended claims contain various words and lettering inside double brackets, which make the claims confusing. For example in claim 14 the third line contains "[[and]] a card number", also in claim 14, lines 12-13 contains "[[a]] the secret key [[K1]] Ki". Numerous examples are in the amended claims. The examiner assumes the double-bracketed text is meant to be deleted. Appropriate correction is required. Amendments to the claims filed on or after July 30, 2003 must comply with 37 CFR 1.121(c) which states:

(c) *Claims.* Amendments to a claim must be made by rewriting the entire claim with all changes (e.g., additions and deletions) as indicated in this subsection, except when the claim is being canceled. Each amendment document that includes a change to an existing claim, cancellation of an existing claim or addition of a new claim, must include a complete listing of all claims ever presented, including the text of all pending and withdrawn claims, in the

Art Unit: 2134

application. The claim listing, including the text of the claims, in the amendment document will serve to replace all prior versions of the claims, in the application. In the claim listing, the status of every claim must be indicated after its claim number by using one of the following identifiers in a parenthetical expression: (Original), (Currently amended), (Canceled), (Withdrawn), (Previously presented), (New), and (Not entered).

(1) *Claim listing.* All of the claims presented in a claim listing shall be presented in ascending numerical order. Consecutive claims having the same status of "canceled" or "not entered" may be aggregated into one statement (e.g., Claims 1–5 (canceled)). The claim listing shall commence on a separate sheet of the amendment document and the sheet(s) that contain the text of any part of the claims shall not contain any other part of the amendment.

(2) *When claim text with markings is required.* All claims being currently amended in an amendment paper shall be presented in the claim listing, indicate a status of "currently amended," and be submitted with markings to indicate the changes that have been made relative to the immediate prior version of the claims. The text of any added subject matter must be shown by underlining the added text. The text of any deleted matter must be shown by strike-through except that double brackets placed before and after the deleted characters may be used to show deletion of five or fewer consecutive characters. The text of any deleted subject matter must be shown by being placed within double brackets if strike-through cannot be easily perceived. Only claims having the status of "currently amended," or "withdrawn" if also being amended, shall include markings. If a withdrawn claim is currently amended, its status in the claim listing may be identified as "withdrawn—currently amended."

(3) *When claim text in clean version is required.* The text of all pending claims not being currently amended shall be presented in the claim listing in clean version, i.e., without any markings in the presentation of text. The presentation of a clean version of any claim having the status of "original," "withdrawn" or "previously presented" will constitute an assertion that it has not been changed relative to the immediate prior version, except to omit markings that may have been present in the immediate prior version of the claims of the status of "withdrawn" or "previously presented." Any claim added by amendment must be indicated with the status of "new" and presented in clean version, i.e., without any underlining.

(4) *When claim text shall not be presented; canceling a claim.*

(i) No claim text shall be presented for any claim in the claim listing with the status of "canceled" or "not entered."

(ii) Cancellation of a claim shall be effected by an instruction to cancel a particular claim number. Identifying the status of a claim in the claim listing as "canceled" will constitute an instruction to cancel the claim.

(5) *Reinstatement of previously canceled claim.* A claim which was previously canceled may be reinstated only by adding the claim as a "new" claim with a new claim number.

Response to Arguments

5. Applicant's arguments with respect to claims 14-26 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language

7. **Claims 19-22, and 26** are rejected under 35 U.S.C. 102(e) as being anticipated by Maruyama et al. U.S. Patent No. 5,883,960 (hereinafter '960).

As to independent claim 19, "A chip having a memory range, wherein at the manufacturer for pre-personalizing the chip a subscriber identification number (IMSI), a card number (ICCID), and an additional secret key Ki are stored" is taught in '960 col. 8, lines 21-29;

"wherein the chip itself derives an initial secret key Ki_1 and," is shown in '960 col. 14, lines 42-55;

"wherein the chip in the terminal equipment is Toolkit-enabled and includes means for communicating with a security center (SC) and negotiating a new secret key Ki_2" is disclosed in '960 col. 14, line 63 through col. 15, line9.

Art Unit: 2134

As to dependent claim 20, “wherein the chip includes means for receiving data from the security center (SC) and means for writing the received data to the memory” is taught in ‘960 col. 3, lines 49-63.

As to dependent claim 21, “wherein the chip comprises a microprocessor for negotiating a secret key with the security center (SC)” is shown in ‘960 col. 4, lines 6-20.

As to dependent claim 22, “wherein the chip includes a dialing number which is fixedly programmed by the manufacturer” is disclosed in ‘960 col. 13, lines 12-19.

As to dependent claim 26, “wherein the chip includes means for reading data received from the security center (SC) in memory, modifying the data and transmitting the data to the security center (SC)” is taught in ‘960 col. 14, lines 30-64.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

9. **Claim 25** is rejected under 35 U.S.C. 103(a) as being unpatentable over ‘960 as applied to claim 19 in further view of Julin et al.

U.S. Patent No. 5,557,679, (hereinafter ‘679).

Art Unit: 2134

As to dependent claim 25, the following is not taught in '960 **"wherein PIN and PUK default values are stored at the chip"** however '679 teaches "" in col. 3, lines 24-35 "Each retailer has data terminal equipment 9, to which are connected a reader 10 for SIM cards 11 and line encryption equipment 12, 13 consisitng For generating IMSI, Ki, and PUK".

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify a method for personalizing an IC card used for mobile communications to include a means to personalize an unblocking. One of ordinary skill in the art would have been motivated to perform such a modification because the personal unblocking key adds to the safety is an essential procedure see '679 (col. 1, lines 20 et seq.) "In mobile telephone systems, in which the mobile units are controlled by active cards assigned to the subscribers, the personalization of the respective card constitutes an essential procedure".

10. **Claims 14, 15, 23, and 24** are rejected under 35 U.S.C. 103(a) as being unpatentable over '960 as applied to claim 14 in further view of '679.

As to independent claim 14, "A, method for personalizing GSM chips" is taught in '960 col. 4, lines 6-9;

"wherein at the manufacturer for pre--personalizing the chip a subscriber identification number (IMSI), a card number (ICCID) and an additional secret key Ki are stored, are stored, comprising the steps of:" is shown in '960 col. 8, lines 21-29;

Art Unit: 2134

“a) performing the personalization of the chip when the subscriber logs on to the subscriber network for the first time” is disclosed in ‘960 col. 12, line 57 through col. 13, line 5;

“b) obtaining the (ICCID) card number and the (IMSI) subscriber identification number from a number pool, the chip itself derives an initial secret; key Ki_1 from the. secret key Ki which is known and entered into the chip” is taught in ‘960 col. 14, lines 42-55;

“c) making an entry in an authentication center (AC) and [[the]] a home location register (HLR) as soon as the subscriber has entered into a contract with a network operator; d) deriving at the authentication center (AC) the initial secret key Ki_1 ; e) setting the conditions of the network so that during logon to the network, a connection is established from the chip to the security center (SC) of the network operator; f) routing the connection from the chip to the security center (SC) during the first logon” is shown in ‘960 col. 21, line 19 through col. 22, line 7;

“g) negotiating between the chip and the security center (SC) a new second secret key Ki_2 ” is disclosed in ‘960 col. 14 line 63 through col. 15, line 9;

“h) disabling the conditions of step e)” is taught in ‘960 col. 14, lines 3-14;

the following is not taught in ‘960 **“while PIN and PUK are set to a default value”** however ‘679 teaches “Each retailer has data terminal equipment 9, to

Art Unit: 2134

which are connected a reader 10 for SIM cards 11 and line encryption equipment 12, 13 consisitng For generating IMSI, Ki, and PUK” in col. 3, lines 24-35.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify a method for personalizing a IC card used for mobile communications to include a means to personalize an unblocking. One of ordinary skill in the art would have been motivated to perform such a modification because ... see ‘679 (col. X, lines XX et seq.) “”.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify a method for personalizing an IC card used for mobile communications to include a means to personalize an unblocking. One of ordinary skill in the art would have been motivated to perform such a modification because the personal unblocking key adds to the safety is an essential procedure see ‘679 (col. 1, lines 20 et seq.) “In mobile telephone systems, in which the mobile units are controlled by active cards assigned to the subscribers, the personalization of the respective card constitutes an essential procedure”.

As to dependent claim 15, “wherein the initial secret key Ki_1 which is first stored in the chip, is not transmitted to and stored in the authentication center (AC) before the contract is established” is taught in ‘960 col. 8, lines 21-29.

As to dependent claim 23, “wherein PIN and PUK default values are stored at the chip” is shown in ‘679 col. 3, lines 24-35.

As to dependent claim 24, “wherein step g) further comprises negotiating at the security center (SC) the PUK with the chip or generated

Art Unit: 2134

in the security center (SC) and transmitted to the chip” is disclosed in '679 col. 3, lines 24-35.

11. **Claims 16-18**, are rejected under 35 U.S.C. 103(a) as being unpatentable over '960 as applied to claim 14 in further view of '679 in further view of Brown et al. U.S. Patent No. 5,793,866 (hereinafter '866).

As to independent claim 16, the following is not taught in the combination of teachings of '960 and '679 **“further comprising the step of employing a Diffie Hellman method to negotiate the second secret key Ki_2”** however '866 teaches “Those skilled in the art will recognize that the above RSA public key cryptography examples are not restrictive, as the methods disclosed may be applied to other techniques. For example, the methods may also be used to provide improved security in Diffie-Hellman (DH) public key cryptography. In DH techniques, a pair of signals are exchanged between the central site” in col. 10 lines 9-15.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify a method for personalizing a IC card used for mobile communications that has a means to personalize an unblocking to include various well-known encryption methods. One of ordinary skill in the art would have been motivated to perform such a modification because an improved method to provide security protection is needed see '866 (col. 1, lines 64 et seq.) “Although the public key exchange is impervious to simple interception, it is vulnerable to a so-called “man –in the-middle” attack”.

Art Unit: 2134

As to dependent claim 17, “wherein the home location register (HLR) is capable of setting and deleting a rerouting command (hotlining flag)” is shown in ‘866 col. 6 lines 15-23.

As to dependent claim 18, “wherein, when the initial secret key Ki₁ is entered into the authentication center (AC) for the first time, the hotlining flag is also set in the home location register (HLR)” is disclosed in ‘866 col. 4 lines 39-60.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a). A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

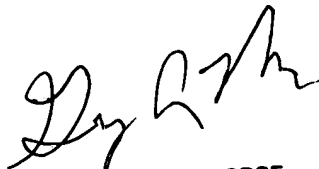
12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (703) 305-8917. The examiner can normally be reached on 6:30 am to 3:30 pm Monday - Thursday and alternating Fridays.

Art Unit: 2134

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A Morse can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Ellen. Tran
Patent Examiner
Technology Center 2134
24 June, 2004


GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2134